ATTACHMENT A

B4

SET Secure Electronic Transaction Specification

Book 1: Business Description

Version 1.0
May 31, 1997

PC

3 Concepts

3.1 Payment System Participants

Interaction of participants

SET changes the way that participants in a payment system interact. In a face-to-face retail transaction or a mail order transaction, electronic processing begins with the merchant or the Acquirer. However, in a SET transaction, the electronic processing begins with the cardholder.

Cardholder

In the electronic commerce environment, consumers and corporate purchasers interact with merchants from personal computers. A cardholder uses a payment card that has been issued by an Issuer. SET ensures that in the cardholder's interactions with the merchant, the payment card account information remains confidential.

Issuer

An Issuer is a financial institution that establishes an account for a cardholder and issues the payment card. The Issuer guarantees payment for authorized transactions using the payment card in accordance with payment card brand regulations and local legislation.

Merchant

A merchant offers goods for sale or provides services in exchange for payment. With SET, the merchant can offer its cardholders secure electronic interactions. A merchant that accepts payment cards must have a relationship with an Acquirer.

Acquirer

An Acquirer is the financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

Payment gateway

A payment gateway is a device operated by an Acquirer or a designated third party that processes merchant payment messages, including payment instructions from cardholders.

Continued on next page

Brand

Financial institutions have founded payment card brands that protect and advertise the brand, establish and enforce rules for use and acceptance of their payment cards, and provide networks to interconnect the financial institutions.

Other brands are owned by financial services companies that advertise the brand, and establish and enforce rules for use and acceptance of their payment cards. These brands combine the roles of Issuer and Acquirer in interactions with cardholders and merchants.

Third parties

Issuers and Acquirers sometimes choose to assign the processing of payment card transactions to third-party processors. This document does not distinguish between the financial institution and the processor of the transactions.

3.2 Cryptography

Protection of sensitive information

Cryptography has been used for centuries to protect sensitive information as it is transmitted from one location to another. In a cryptographic system, a message is encrypted using a key. The resulting ciphertext is then transmitted to the recipient where it is decrypted using a key to produce the original message. There are two primary encryption methods in use today: secret-key cryptography and public-key cryptography. SET uses both methods in its encryption process.

Secret-key cryptography

Secret-key cryptography, also known as symmetric cryptography, uses the same key to encrypt and decrypt the message. Therefore, the sender and the recipient of a message must share a secret, namely the key. A well known secret-key cryptography algorithm is the Data Encryption Standard (DES), which is used by financial institutions to encrypt PINs (personal identification numbers).

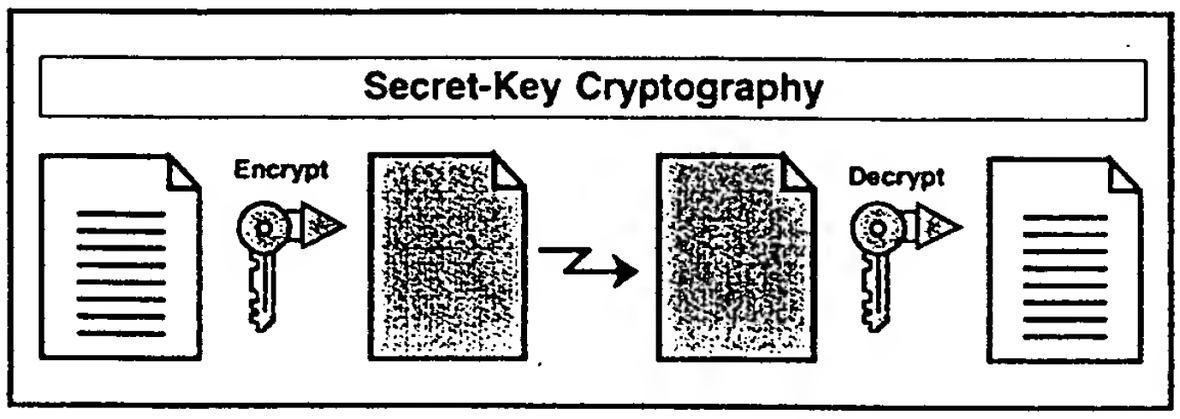

Figure 1: Secret-Key Cryptography

Continued on next page

3.2 Cryptography, continued

Public-key cryptography

Public-key cryptography, also known as asymmetric cryptography, uses two keys: one key to encrypt the message and the other key to decrypt the message. The two keys are mathematically related so that data encrypted with either key can only be decrypted using the other. Each user has two keys: a *public key* and a *private key*. The user distributes the public key. Because of the relationship between the two keys, the user and anyone receiving the public key can be assured that data encrypted with the public key and sent to the user can only be decrypted when the user uses the private key. *This assurance is only maintained if the user ensures that the private key is not disclosed to anyone else.* Therefore, the key pair should be generated by the user. The best known public-key cryptography algorithm is RSA (named after its inventors Rivest, Shamir, and Adleman).

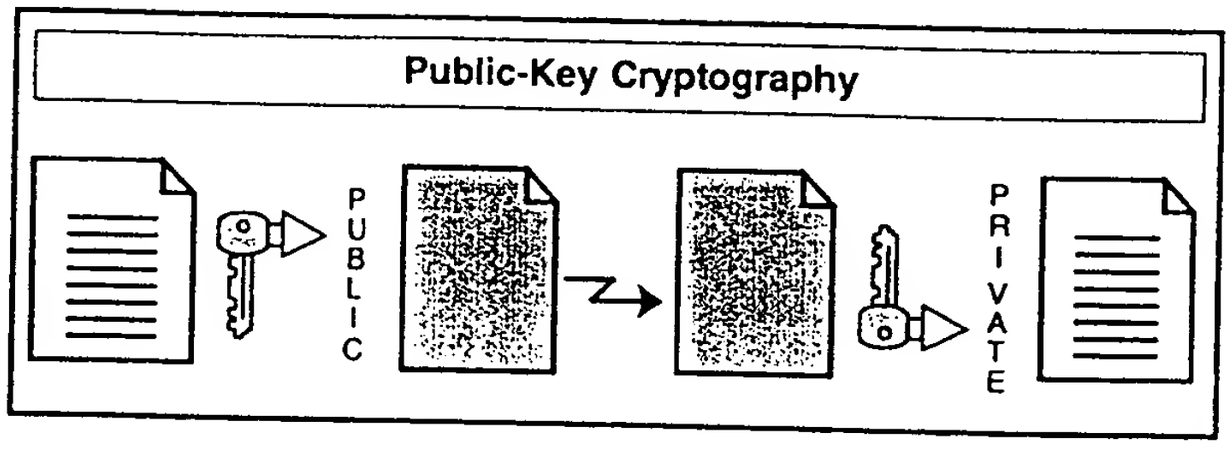

Figure 2: Public-Key Cryptography

Secret-key cryptography is impractical for exchanging messages with a large group of previously unknown correspondents over a public network. For a merchant to conduct transactions securely with millions of Internet subscribers, each consumer would need a distinct key assigned by that merchant and transmitted over a separate secure channel. On the other hand, by using public-key cryptography, that same merchant could create a public/private key pair and publish the public key, allowing any consumer to send a secure message to that merchant.

Continued on next page